

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

Date filed: February 8, 2019

Name of company covered by this certification: Alenco Communications, Inc. d/b/a ACI

Form 499 Filer ID: 802461

Name of signatory: Ray Bussell

Title of signatory: General Manager

I, Ray Bussell, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company *is* in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company *has not* taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company *has not* received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

A handwritten signature in blue ink, appearing to read "Ray Bussell", is written over a horizontal line.

Attachment: Accompanying Statement explaining CPNI procedures

ACCOMPANYING STATEMENT

To the best of my knowledge, Alenco Communications, Inc. d/b/a ACI (“the Company”) is in full compliance with the FCC rules on CPNI and its requirements for the safeguarding of such customer information. The Company’s operating procedures ensure that it is in compliance with the FCC’s CPNI rules because disclosure of, or permitting access to, our customers’ CPNI is not allowed without obtaining the requisite customer approval, except as required by law, or the exceptions set forth in 47 U.S.C. §222, and Subpart U of Title 47 of the Code of Federal Regulations; 47 C.F.R §64.2001 through §64.2011.

The Company has internal procedures in place to educate our employees about CPNI and the disclosure of CPNI. Employees with access to this information are aware of the FCC’s rules and are prohibited from disclosing or permitting access to CPNI without the appropriate customer consent or as allowed by law and the FCC rules. Any employee that accesses, discloses, or uses CPNI in violation of federal regulations is subject to disciplinary action, and possible termination.

The Company has assigned a Director for CPNI Compliance to serve as the central point of contact regarding the Company’s CPNI responsibilities and questions related to CPNI Policy. The Director for CPNI Compliance has responsibilities including, but not limited to, supervising the training of all Company employees with access to CPNI, investigating complaints of unauthorized release of CPNI, and reporting any breaches to the appropriate law enforcement agencies. The Director for CPNI Compliance also maintains records in accordance with FCC CPNI rules, including records of any discovered breaches, notifications of breaches to law enforcement, and law enforcements’ responses to the notifications for a period of at least two years.

Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with C.F.R. §64.2010. Prior to the disclosure of CPNI, customers initiating calls to, or visiting the Company’s offices, are properly authenticated. Passwords and password back-up authentication procedures for lost or forgotten passwords are implemented in accordance with §64.2010(e). To establish a password for an existing customer, the Company must first authenticate the customer without the use of readily available biographical information or account information, such as calling the customer back at their telephone number of record. For a new customer, the password would be established at the time of service initiation.

ACCOMPANYING STATEMENT (Continued)

Call detail information is only disclosed over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the Company asking for readily available biographical information or account information. If the customer does not provide a password, call detail information is only provided by sending it to the customer's address of record or by calling the customer at their telephone number of record. If the customer is able to provide call detail information to the Company during a customer-initiated call without the Company's assistance, then the Company is permitted to discuss the call detail information provided by the customer. Prior to the Company disclosing CPNI to a customer visiting any of its retail offices in person, the customer must present a valid photo ID matching the customer's account information.

The Company does not rely on readily available biographical information or account information to authenticate a customer's identity before a customer can access CPNI related to their telecommunications account online. Once authenticated, a customer can only obtain online access to CPNI related to his or her telecommunications account with a password that is not prompted by the Company asking for readily available biographical information or account information.

The Company has implemented procedures to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record is created or changed.

The Company provides notice to the customer of their right to restrict use of disclosure of, and access to, that customer's CPNI. The Company uses the opt-out method to solicit approval to use its customer's individually identifiable CPNI for the purpose of marketing communications-related services in compliance with §§ 64.2007 and 64.2008. The Company is aware of the requirement that notice is to be provided to the Commission within five business days of any instances where the opt-out mechanism does not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly. However, no circumstances have yet required such a notification by the Company. Supervisory approval must be obtained of any proposed outbound marketing request for customer approval.

The Company requires express opt-in consent from a customer prior to the release of CPNI to a joint venture partner or independent contractor for marketing purposes. However, currently the Company has not and does not plan to use, sell, or release CPNI to any third parties for marketing purposes which require opt-in consent.